

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A system, comprising:
 - a client workstation;
 - a single sign-on ("SSO") server accessible to the client workstation;
 - a plurality of host servers accessible to the client workstation, a unique public key being associated with each host server;
wherein access by the client workstation to a first host server causes the client workstation to be automatically re-directed to the SSO server and the SSO server causes the client workstation to request sign-on credentials from a user if the user has not signed on to any of the host servers, and wherein the first host server, not the SSO server, authenticates the user; and
wherein said sign-on credentials are used to authenticate the user upon accessing each host server, and wherein said sign-on credentials are encrypted with the public key associated with the host server for which the sign-on credentials were most recently used to authenticate the user.
2. (Currently amended) The ~~computer~~-system of claim 1 wherein, upon being re-directed to the SSO server, the first host server supplies the SSO server with security information that is used to encrypt sign-on credentials.
3. (Currently amended) The ~~computer~~-system of claim 1 wherein the user's sign-on credentials are stored in the client workstation.

4. (Currently amended) The ~~computer~~-system of claim 1 wherein the user's sign-on credentials are stored in the SSO server.
5. (Currently amended) The ~~computer~~-system of claim 3 wherein, after the first host server authenticates the user, the client workstation accesses a second host server which causes the client workstation to be automatically re-directed to the SSO server, and wherein the SSO server causes the sign-on credentials to be retrieved and used by the second host server to authenticate the user without the user supplying additional sign-on credentials.
6. (Currently amended) The ~~computer~~-system of claim 1 wherein the user's sign-on credentials are stored in a cookie in the client workstation.
7. (Currently amended) The ~~computer~~-system of claim 1 wherein the user's sign-on credentials are stored in encrypted form in a cookie in the client workstation.
8. (Currently amended) The ~~computer~~-system of claim 1 wherein, after requesting sign-on credentials from the user, the client workstation is automatically re-directed back to the first host server to authenticate the user.
9. (Currently amended) A client workstation configured to access any one or more of a plurality of services, comprising:
 - a CPU;
 - an input device coupled to the CPU; and
 - storage coupled to the CPU, said storage containing a browser that is executed by the CPU and that causes the workstation to:
 - browse to a service that runs in a host server;
 - automatically re-direct to a single sign-on ("SSO") server; and
 - permit the host server to authenticate a user either by requiring the user to enter credentials via the input device if the user has

not already signed-on to a service and providing the credentials to the host server or, without the user entering credentials, by providing credentials previously stored in the storage to the host server if the user has already signed-on to a service and providing the credentials to the host server;

wherein said credentials are encrypted using a public key associated with the host server that the client workstation most recently accessed.

10. (Original) The client workstation of claim 9 wherein the CPU further causes the workstation to be re-directed back to the service to permit the host server to authenticate the user.

11. (Currently amended) The client workstation of claim 9 wherein the credentials are encrypted and stored in the storage.

12. (Canceled).

13. (Currently amended) A single sign-on (“SSO”) server, comprising:
a CPU;
storage coupled to the CPU, said storage containing software that is executed by the CPU and that causes the SSO server to:
cause user credentials to be entered by a user of a first computer if the user has not already signed-on to a service and to be encrypted using a first public key associated with a host computer, or to cause user credentials previously stored in the first computer to be retrieved, decrypted, and then encrypted using a second public key associated with a second computer, the first public key being different than the second public key; and

cause the user credentials to be used by [[a]] the second computer to authenticate the user.

14. (Canceled).

15. (Canceled).

16. (Currently amended) A host computer on which a user accessible service is executed, comprising:

a CPU; and

software executable by said CPU;

wherein the CPU causes a user's browser to be re-directed to a first computer to obtain user credentials and that causes a user's browser to be re-directed back to the host computer so that the host computer can authenticate the user using the credentials;

wherein the CPU decrypts the credentials using a private key associated with the host computer.

17. (Canceled).

18. (Currently amended) A system, comprising:

means for providing user identifying information from a user if the user has not already signed-on to a service;

means for retrieving user identifying information previously stored in a computer if the user has already signed-on to a service; and

means for hosting a service and for authenticating the user using the user identifying information; and

means for encrypting user credentials using a public key associated with a means for hosting, a different public key being associated with each of multiple means for hosting.

Appl. No. 10/773,973
Amdt. dated August 1, 2007
Reply to Office Action of May 1, 2007

19. (Original) The system of claim 18 further comprising means for generating a cookie that contains the user identifying information and for storing the cookie in a user-controlled computer.
20. (Currently amended) A method, comprising:
accessing a host server;
automatically re-directing from the host server to a sign-on server;
either retrieving previously stored user credentials if a user has already accessed a service or requesting the user to enter user credentials if the user has not already accessed a service;
re-directing back to the host server; and
the host server authenticating the user using the user credentials; and
encrypting said user credentials with a public key associated with the host
server that the user most recently accessed, a different public key
being associated with each of multiple host servers.
21. (Canceled).
22. (Original) The method of claim 20 further comprising storing user-entered user credentials in a computer that is controllable by the user and that is not the sign-on server.
23. (Original) The method of claim 22 wherein storing the user credentials comprises storing the user credentials in a cookie that is stored in the computer.
24. (Original) The method of claim 20 further comprising, upon re-directing to the sign-on server, determining whether the user has already accessed a service.